

**IEEE 802.11N
WIRELESS OUTDOOR CPE
User's Manual**

V2.0 June 2010

Copyright

Copyright © 2010 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual is intended to guide professional installer to install the IEEE 802.11N WIRELESS OUTDOOR CPE Wireless CPE and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:



Note:

-
- This indicates an important note that you must pay attention to.
-



Warning:

-
- This indicates a warning or caution that you have to abide.
-

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

To avoid the possibility of exceeding radio frequency exposure limits, you shall keep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Warranty

Standard hardware warranty is for one (1) year from date of shipment from Distributor. Warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

IN NO EVENT SHALL DISTRIBUTOR BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL DISTRIBUTOR LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Content

Chapter 1 Introduction.....	1
Introduction	1
Appearance	2
Key Features	2
Typical Application	3
Chapter 2 Hardware Installation	4
Preparation before Installation.....	4
Professional Installation Required	4
Safety Precautions.....	4
Installation Precautions.....	5
Product Package.....	5
Hardware Installation	7
Connect up.....	7
Pole Mounting	10
Using the External Antenna	12
Chapter 3 Basic Settings.....	14
Factory Default Settings	14
System Requirements	15
How to Login the Web-based Interface	15
Basic System Settings.....	17
RADIUS Settings	20
Time Settings.....	21
Firewall Settings	22
Basic Wireless Settings.....	26
Site Survey	28
Chapter 4 Advanced Settings	30
Advanced Wireless Settings.....	30

Wireless Security Settings	33
Security Settings	33
Access Control	35
WDS Settings	36
Chapter 5 Management.....	37
SNMP Management	37
Configure SNMPv3 User Profile	38
Password	39
Upgrade Firmware	40
Backup/ Retrieve Settings	40
Restore Factory Default Settings	41
Reboot	42
System Log	42
Site Survey	43
Ping Watch Dog	44
Chapter 6 Status	45
View IEEE 802.11N WIRELESS OUTDOOR CPE Basic Information	45
View Association List	45
View Network Flow Statistics	46
View Bridge Table	46
View ARP Table	47
View Active DHCP Client Table	48
Chapter 7 Troubleshooting	49
Appendix A. ASCII	51
Appendix B. GPL Declamation	52

FIGURE

Figure 1 IEEE 802.11N WIRELESS OUTDOOR CPE.....	2
Figure 2 Typical Application	3
Figure 3 Move the Cover.....	7
Figure 4 Cable Connection	7
Figure 5 Seal the Bottom	8
Figure 6 Connect to PoE Injector.....	8
Figure 7 Complete Set	9
Figure 8 Pole Mounting – Step 1	10
Figure 9 Pole Mounting – Step 2.....	10
Figure 10 Pole Mounting – Step 3.....	11
Figure 11 Move the Rubber.....	12
Figure 12 Login Page.....	15
Figure 13 Main Page.....	16
Figure 14 Basic System Settings	17
Figure 15 IP Settings (Bridge)	17
Figure 16 IP Settings (Router)	18
Figure 17 RADIUS Settings	20
Figure 18 Time Settings	20
Figure 19 Source IP Filtering	21
Figure 20 Destination IP Filtering	22
Figure 21 Source Port Filtering	22
Figure 22 Destination Port Filtering	23
Figure 23 Port Forwarding	23
Figure 24 DMZ	24
Figure 25 Basic Wireless Settings	26
Figure 26 Site Survey.....	29
Figure 27 Advanced Wireless Settings	30
Figure 28 Security Settings.....	33
Figure 29 Access Control	35

Figure 30 WDS Settings	34
Figure 31 SNMP Management	35
Figure 32 Configure SNMPv3 User Profile	36
Figure 33 Password	37
Figure 34 Upgrade Firmware	38
Figure 35 Backup/Retrieve Settings	39
Figure 36 Restore Settings	41
Figure 39 Basic Information	45
Figure 40 Connection	45
Figure 41 Network Flow Statistics	46
Figure 42 Bridge Table	44
Figure 43 ARP Table	44
Figure 44 Active DHCP Client Table	45
Figure 45 MAC Address	49

TABLE

Table 1 IEEE 802.11N WIRELESS OUTDOOR CPE Factory Default Settings.....	14
Table 2 ACSII	51
Table 3 Public Software Name and Description	53

Chapter 1 Introduction

Introduction

Designed for outdoor environment application, the IEEE 802.11N WIRELESS OUTDOOR CPE is a high-performance last-mile broadband solution that provides reliable wireless network coverage. As an IEEE 802.11b/g compliant wireless device, the IEEE 802.11N WIRELESS OUTDOOR CPE is able to give stable and efficient wireless performance, while designed with IEEE 802.11n draft 2.0 standard and high output power makes it possible to deliver several times faster data rate than normal wireless device and higher bandwidth with longer range for outdoor applications.

The IEEE 802.11N WIRELESS OUTDOOR CPE supports four wireless communication connectivity (AP, Wireless Client, WDS and AP Repeater), allowing for various application requirements thus helping to find the key to the “last mile” with least effort.

With high output power and reliable performance, the IEEE 802.11N WIRELESS OUTDOOR CPE is an ideal wireless broadband solution for wireless Internet service providers and system integrators!

Appearance



Figure 1 IEEE 802.11N WIRELESS OUTDOOR CPE

Key Features

- Compliant with IEEE 802.11b/g and IEEE 802.11n draft 2.0 as well
- Support Power Through Ethernet which is supplied with 12V.
- High reliable watertight housing endures almost any harsh environments
- Four operating modes including AP, Wireless Client, WDS and AP Repeater
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- User-friendly Web and SNMP-based management interface

Typical Application

This section describes the typical applications of IEEE 802.11N WIRELESS OUTDOOR CPE. By default, it is set to AP mode which allows it to establish a wireless coverage; besides, it is also able to join any available wireless network under wireless client mode. The IEEE 802.11N WIRELESS OUTDOOR CPE is able to deliver stable and efficient broadband connectivity for various applications.

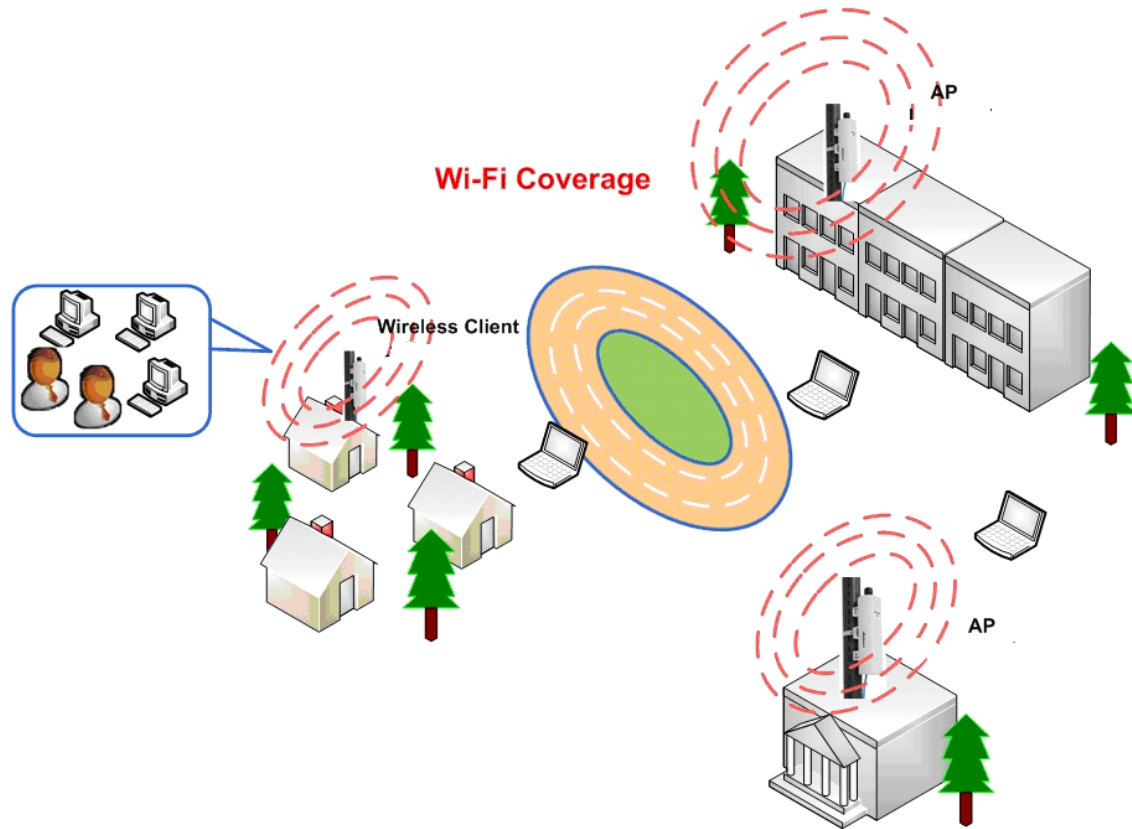


Figure 2 Typical Application

Besides, the IEEE 802.11N WIRELESS OUTDOOR CPE can also be applied into the following environments:

- Cost-effectively provide long distance backhaul for remote areas (e.g. village, oil well, island, mountain and etc.)
- Establish local backhaul for campus, farm and factory
- Provide and access for video streaming or surveillance for industrial and mining enterprises

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing IEEE 802.11N WIRELESS OUTDOOR CPE.

Preparation before Installation

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing IEEE 802.11N WIRELESS OUTDOOR CPE for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing IEEE 802.11N WIRELESS OUTDOOR CPE, please note the following things:
 - ♦ Do not use a metal ladder;
 - ♦ Do not work on a wet or windy day;
 - ♦ Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

Installation Precautions

To keep the IEEE 802.11N WIRELESS OUTDOOR CPE well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed surge arrestor with the IEEE 802.11N WIRELESS OUTDOOR CPE; otherwise, a random lightening could easily cause fatal damage to IEEE 802.11N WIRELESS OUTDOOR CPE. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
2. Users MUST use the “Power cord & PoE Injector” shipped in the box with the IEEE 802.11N WIRELESS OUTDOOR CPE. Use of other options will cause damage to the IEEE 802.11N WIRELESS OUTDOOR CPE.
3. Users MUST power off the IEEE 802.11N WIRELESS OUTDOOR CPE first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the IEEE 802.11N WIRELESS OUTDOOR CPE; otherwise, damage might be caused to the IEEE 802.11N WIRELESS OUTDOOR CPE itself.

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

- | | |
|-------------------------------------|-----|
| • IEEE 802.11N WIRELESS OUTDOOR CPE | × 1 |
| • Pole Mounting Ring | × 1 |
| • Power Cord & PoE Injector | × 1 |
| • Quick Installation Guide | × 1 |
| • Product CD | × 1 |



Note:

-
- Product CD contains Quick Installation Guide and User Manual!
-

Pole Mounting Ring



Power Cord & PoE Injector



Warning:

-
- Users **MUST** use the “Power cord & PoE Injector” shipped in the box with the IEEE 802.11N WIRELESS OUTDOOR CPE. Use of other options will cause damage to the IEEE 802.11N WIRELESS OUTDOOR CPE.
-

Hardware Installation

Connect up

1. The bottom of the IEEE 802.11N WIRELESS OUTDOOR CPE is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.

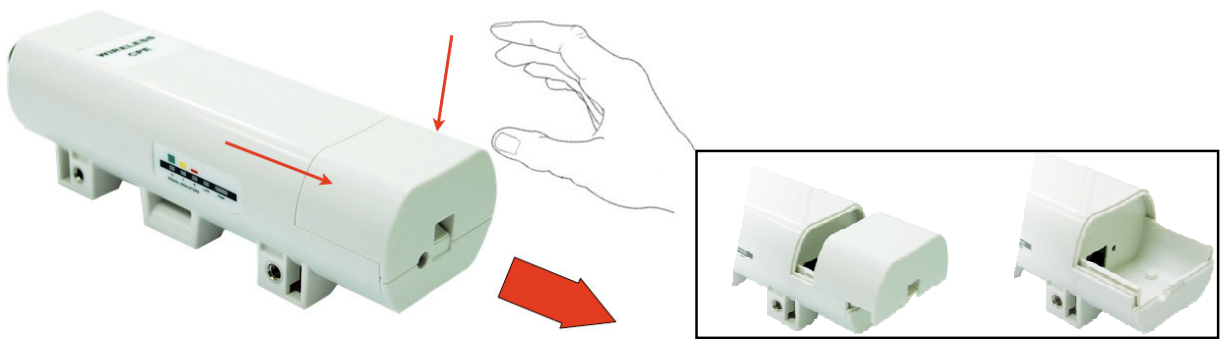


Figure 3 Move the Cover

2. Plug a standard Ethernet cable into the RJ45 port.



Figure 4 Cable Connection

3. Slide the cover back to seal the bottom of the IEEE 802.11N WIRELESS OUTDOOR CPE.



Figure 5 Seal the Bottom

4. Plug the power cord into the DC port of the PoE injector as the following right picture shows.



Figure 6 Connect to PoE Injector

5. Plug the other side of the Ethernet cable as shown in Step 3 into the PoE port of the PoE injector and get the complete set ready.



Figure 7 Complete Set

Pole Mounting

1. Turn the IEEE 802.11N WIRELESS OUTDOOR CPE over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through IEEE 802.11N WIRELESS OUTDOOR CPE as the following right picture shows.

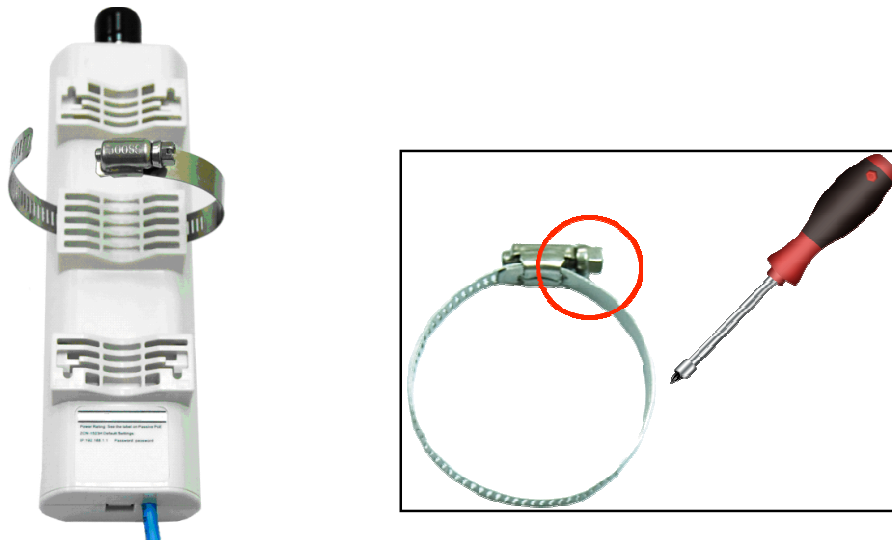


Figure 8 Pole Mounting – Step 1

2. Mount IEEE 802.11N WIRELESS OUTDOOR CPE steadily to the pole by locking the pole mounting ring tightly.



Figure 9 Pole Mounting – Step 2

3. Now you have completed the hardware installation of IEEE 802.11N WIRELESS OUTDOOR CPE.



Figure 10 Pole Mounting – Step 3

Using the External Antenna

If you prefer to use the external antenna with N-type connector for your application instead of the built-in directional antenna, please follow the steps below.

1. Grab the black rubber on the top of IEEE 802.11N WIRELESS OUTDOOR CPE, and slightly pull it up. The metal N-type connector will appear.

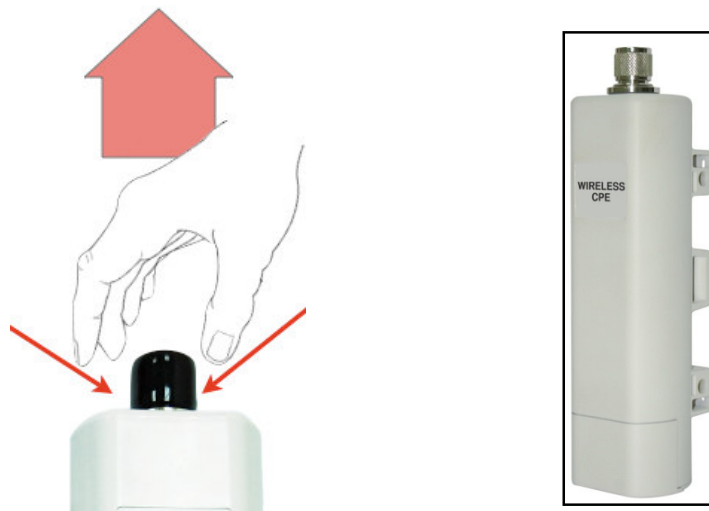


Figure 11 Move the Rubber

2. Connect your antenna with the N-type connector on the top of IEEE 802.11N WIRELESS OUTDOOR CPE.



Note:

- If you are going to use an external antenna on IEEE 802.11N WIRELESS OUTDOOR CPE, get some cable in advance.
- Be aware of the force you use while connecting to the N-type connector, inappropriate force may damage the N-type connector!



Warning:

- Users **MUST** power off the IEEE 802.11N WIRELESS OUTDOOR CPE first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external

antenna onto the IEEE 802.11N WIRELESS OUTDOOR CPE; otherwise, damage might be caused to the IEEE 802.11N WIRELESS OUTDOOR CPE itself.

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the IEEE 802.11N WIRELESS OUTDOOR CPE factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "[Restore Factory Default Settings](#)".

Table 1 IEEE 802.11N WIRELESS OUTDOOR CPE Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
802.11 Mode		802.11b/g/n
Channel Number		6
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel Mode		20MHz
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Security		Open System

Encryption		None
Wireless Separation		Disable
Access Control		Disable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of IEEE 802.11N WIRELESS OUTDOOR CPE is 192.168.1.1. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape or Firefox.

How to Login the Web-based Interface

The IEEE 802.11N WIRELESS OUTDOOR CPE provides you with user-friendly Web-based management tool.

- Open Web browser and enter the IP address (Default: **192.168.1.1**) of IEEE 802.11N WIRELESS OUTDOOR CPE into the address field. You will see the login page as below.



Wireless Broadband Access Point

Name

Password

Figure 12 Login Page

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click “**Login**” to login the main page of IEEE 802.11N WIRELESS OUTDOOR CPE. As you can see, this management interface provides five main options in the black bar above, which are Status, System, Wireless, Management and Tools.

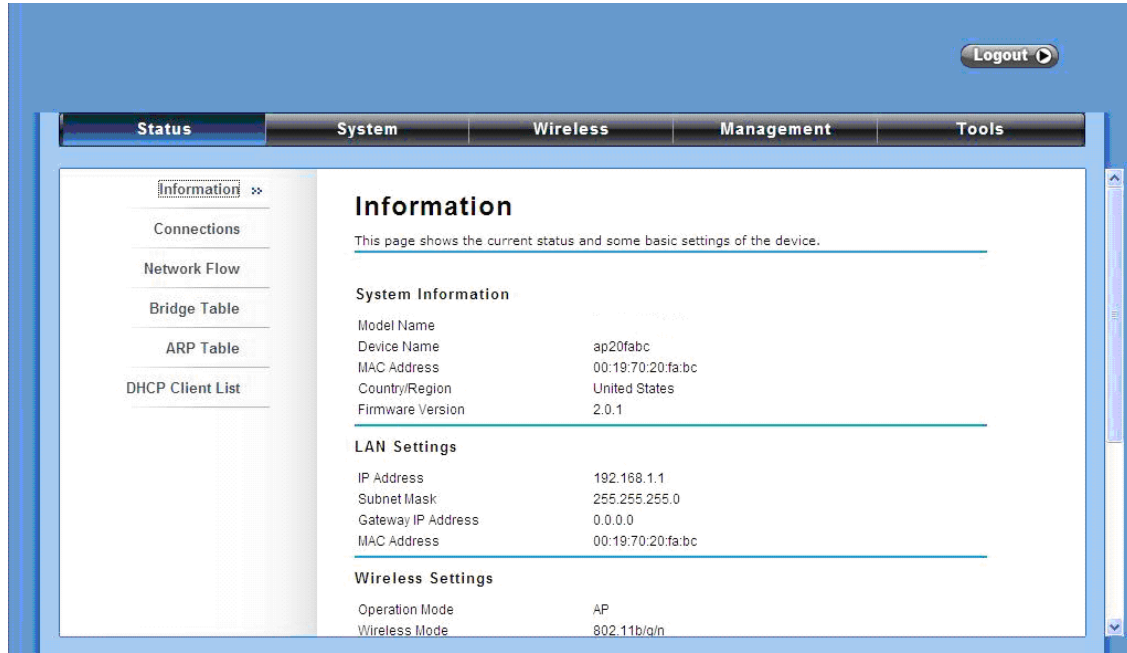


Figure 13 Main Page

 Note:

- The username and password are case-sensitive, and the password should be no more than 19 characters!

Basic System Settings

For users who use the IEEE 802.11N WIRELESS OUTDOOR CPE for the first time, it is recommended that you begin configuration from “**Basic Settings**” in “**System**” shown below:

The screenshot shows a web-based configuration interface for a device. At the top, there is a blue header bar with a "Logout" button on the right. Below the header is a navigation menu with five tabs: "Status", "System", "Wireless", "Management", and "Tools". The "System" tab is currently selected. On the left side of the "System" tab, there is a sub-menu with the following options: "Basic Settings" (which is highlighted with a double arrow), "IP Settings(Bridge)", "IP Settings(Router)", "RADIUS Settings", "Time Settings", and "Firewall Settings". The main content area on the right is titled "Basic Settings". It contains a section labeled "Basic Settings." followed by three configuration fields: "Network Modes:" with a dropdown menu set to "Bridge", "Device Name:" with a text input field containing "ap20fabrc" and a note "(max. 15 characters and no spaces)", and "Country/Region:" with a dropdown menu set to "United States". At the bottom of this section are two buttons: "Apply" and "Cancel".

Figure 14 Basic System Settings

- **Basic Settings**

Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to “**IP Settings (Router)**”.

Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Country Region: The availability of some specific channels and/or operational frequency bands is country dependent.

- **IP Settings (Bridge)**

This is available only under Bridge network mode. Open “**IP Settings (Bridge)**” in “**System**” as below to configure the parameters for LAN which connects to the LAN port of IEEE 802.11N WIRELESS OUTDOOR CPE. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

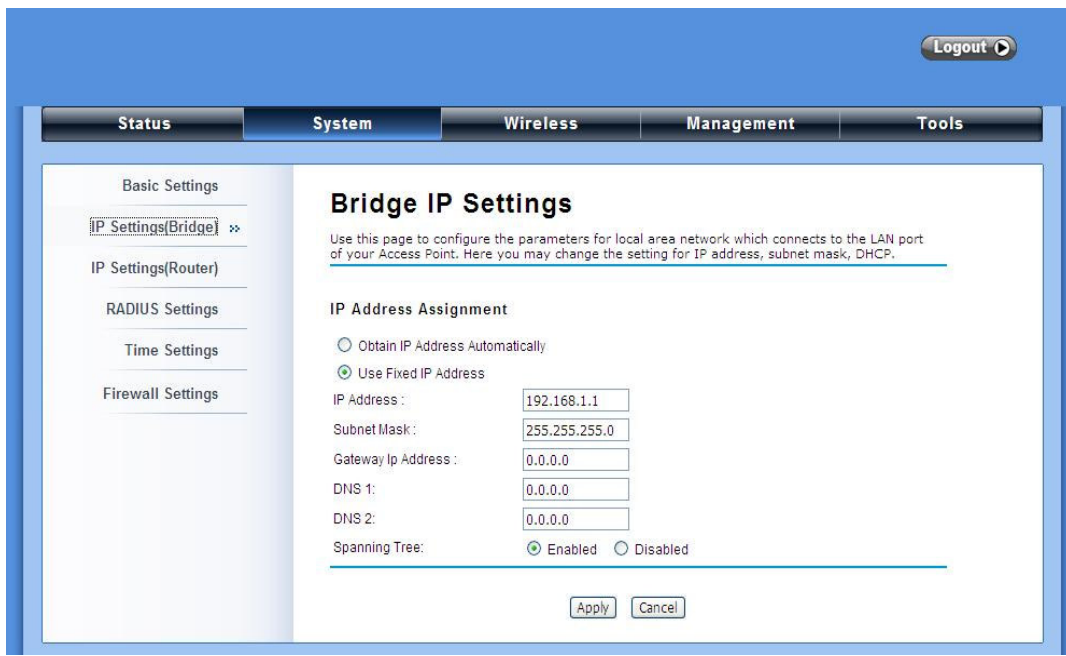


Figure 15 IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the IEEE 802.11N WIRELESS OUTDOOR CPE is able to obtain IP settings automatically from that DHCP server.

Note: When the IP address of the IEEE 802.11N WIRELESS OUTDOOR CPE is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the client computer by running the “nbtstat -r” command before using the device name of the IEEE 802.11N WIRELESS OUTDOOR CPE to access its Web Management page.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for IEEE 802.11N WIRELESS OUTDOOR CPE manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

- **IP Settings (Router)**

This is available only under Router mode. Open “**IP Settings (Router)**” in “**System**” below to

Chapter 3 Basic Settings Page 18

configure the parameters of IEEE 802.11N WIRELESS OUTDOOR CPE for accessing the Internet.

Figure 16 IP Settings (Router)

WAN Settings: Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for IEEE 802.11N WIRELESS OUTDOOR CPE manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes).



Warning:

- In AP mode, IEEE 802.11N WIRELESS OUTDOOR CPE must establish connection with another wireless device before it is set to Router mode. In Router mode, it is impossible for users to access device via wired port, for WAN is on wired port and LAN is on wireless port. Users can access device through the wireless device connected with IEEE 802.11N WIRELESS OUTDOOR CPE.
- In CPE mode, users can access IEEE 802.11N WIRELESS OUTDOOR CPE via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to

Router mode.

- Bridge mode and AP Repeater mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect IEEE 802.11N WIRELESS OUTDOOR CPE with another wireless device before it is set to Router mode and access IEEE 802.11N WIRELESS OUTDOOR CPE via the connected wireless device.
-

RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open “**RADIUS Settings**” in “**System**” to make RADIUS configuration.

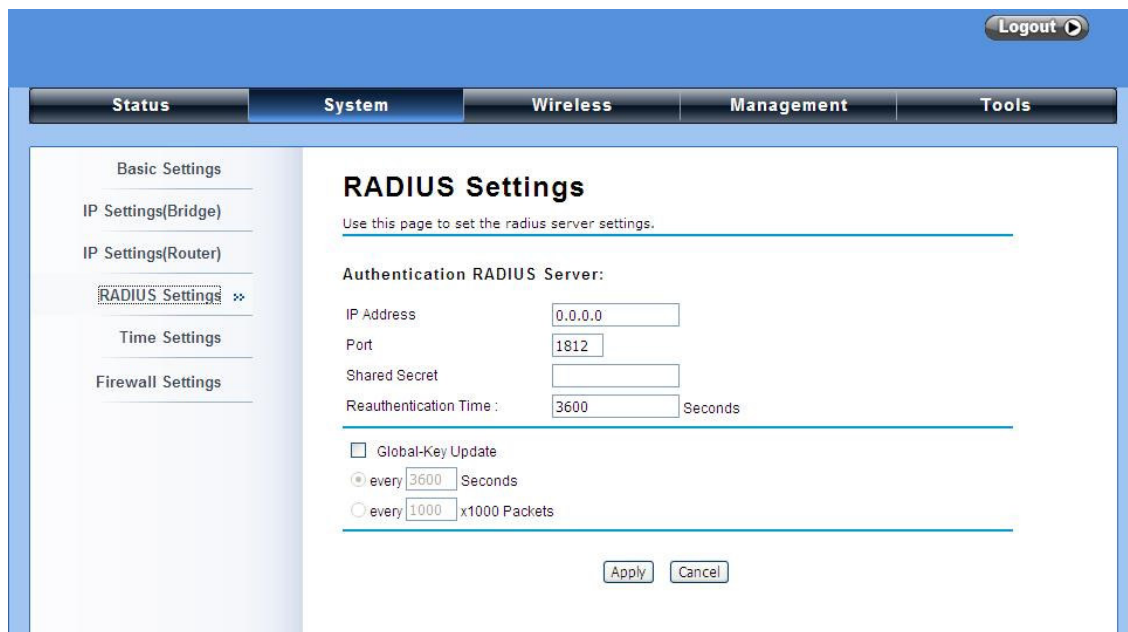


Figure 1715 RADIUS Settings

- **Authentication RADIUS Server**

This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

IP Address: Enter the IP address of the Radius Server;

Port: Enter the port number of the Radius Server;

Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the IEEE 802.11N WIRELESS OUTDOOR CPE and RADIUS during authentication.

Re-authentication Time: Set the time interval between two authentications.

Global-Key Update: Check this option and specify the time interval between two global-key updates.

Time Settings

Compliant with NTP, the IEEE 802.11N WIRELESS OUTDOOR CPE is capable of keeping its time in complete accord with the Internet time. Make configuration in “**Time Settings**” from “**System**”. To use this feature, check “**Enable NTP Client Update**” in advance.

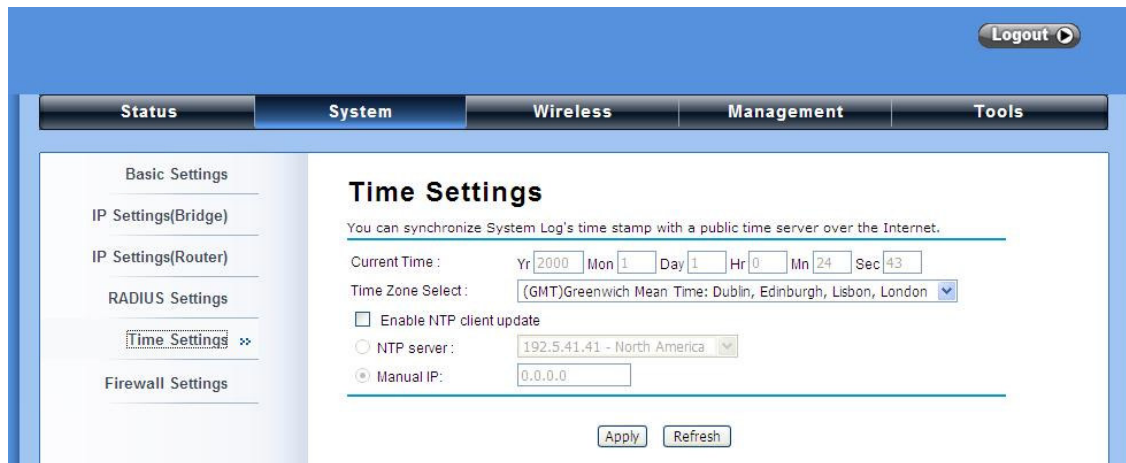
The screenshot shows a web interface for configuring system settings. At the top, there is a blue header bar with a 'Logout' button. Below the header is a navigation menu with tabs for 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is selected. On the left side, there is a sidebar menu with options: 'Basic Settings', 'IP Settings(Bridge)', 'IP Settings(Router)', 'RADIUS Settings', 'Time Settings' (which is highlighted with a double arrow), and 'Firewall Settings'. The main content area is titled 'Time Settings' and contains the following fields: 'Current Time' with input boxes for Year (2000), Month (1), Day (1), Hour (0), Minute (24), and Second (43); 'Time Zone Select' with a dropdown menu showing '(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'; an 'Enable NTP client update' checkbox; an 'NTP server' dropdown menu showing '192.5.41.41 - North America'; and a 'Manual IP' input box with '0.0.0.0'. At the bottom of the form are 'Apply' and 'Refresh' buttons.

Figure 18 Time Settings

- **Current Time**

Display the present time in Yr, Mon, Day, Hr, Min and Sec.A

- **Time Zone Select**

Select the time zone from the dropdown list.

- **NTP Server**

Select the time server from the “**NTP Server**” dropdown list or manually input the IP address of available time server into “**Manual IP**”.

Hit “**Apply**” to save settings.

Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. IEEE 802.11N WIRELESS OUTDOOR CPE has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under Router Mode.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through IEEE 802.11N WIRELESS OUTDOOR CPE. Use of such filters can be helpful in securing or restricting your local network.

The screenshot shows a web interface for configuring Source IP Filtering. At the top, there is a 'Logout' button. Below it is a navigation bar with tabs: 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is selected. On the left side, there is a sidebar menu with the following items: 'Basic Settings', 'IP Settings(Bridge)', 'IP Settings(Router)', 'RADIUS Settings', 'Time Settings', 'Firewall Settings', 'Src IP Filtering' (which is highlighted with a double arrow), 'Dest IP Filtering', 'Src Port Filtering', 'Dest Port Filtering', 'Port Forwarding', and 'DMZ'. The main content area is titled 'Source IP Filtering'. It contains a text box explaining that entries in the table are used to restrict data packets from the local network to the Internet. Below this, there is a checkbox labeled 'Enable Source IP Filtering'. Underneath the checkbox, there are two input fields: 'Local IP Address:' and 'Comment:'. To the right of these fields are 'Apply' and 'Cancel' buttons. Below the input fields, there is a section titled 'Current Filter Table:' which contains a table with four columns: 'Local IP Address', 'Comment', 'Select', and 'Edit'. Below the table, there are three buttons: 'Delete Selected', 'Delete All', and 'Cancel'.

Figure 19 Source IP Filtering

Destination IP Filtering: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Check the “Enable Source IP Filtering” checkbox and enter the IP address of the clients to be restricted. Hit **Apply** to make the setting take effect.

The screenshot shows the 'Destination IP Filtering' configuration page. The left sidebar contains a menu with options: Basic Settings, IP Settings(Bridge), IP Settings(Router), RADIUS Settings, Time Settings, Firewall Settings, Src IP Filtering, Dest IP Filtering (selected), Src Port Filtering, Dest Port Filtering, and Port Forwarding. The main content area has a title 'Destination IP Filtering' and a description: 'Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.' Below this is a checkbox 'Enable Destination IP Filtering'. There are input fields for 'Destination IP Address' and 'Comment'. At the bottom, there is a table titled 'Current Filter Table' with columns: Destination IP Address, Comment, Select, and Edit. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Cancel'. There are also 'Apply' and 'Cancel' buttons above the table.

Figure 20 Destination IP Filtering

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through IEEE 802.11N WIRELESS OUTDOOR CPE. Use of such filters can be helpful in securing or restricting your local network.

The screenshot shows the 'Source Port Filtering' configuration page. The left sidebar contains a menu with options: Basic Settings, IP Settings(Bridge), IP Settings(Router), RADIUS Settings, Time Settings, Firewall Settings, Src IP Filtering, Dest IP Filtering, Src Port Filtering (selected), Dest Port Filtering, and Port Forwarding. The main content area has a title 'Source Port Filtering' and a description: 'Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' Below this is a checkbox 'Enable Source Port Filtering'. There are input fields for 'Port Range' (with a dropdown for 'Both'), 'Protocol', and 'Comment'. At the bottom, there is a table titled 'Current Filter Table' with columns: Source Port Range, Protocol, Comment, Select, and Edit. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Cancel'. There are also 'Apply Changes' and 'Cancel' buttons above the table.

Figure 21 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through IEEE 802.11N WIRELESS OUTDOOR CPE. Use of such filters can be helpful in securing or restricting your local network.

The screenshot shows a web interface for configuring a wireless outdoor CPE. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A 'Logout' button is in the top right. The left sidebar lists various settings: Basic Settings, IP Settings(Bridge), IP Settings(Router), RADIUS Settings, Time Settings, Firewall Settings, Src IP Filtering, Dest IP Filtering, Src Port Filtering, Dest Port Filtering (highlighted with a double arrow), and Port Forwarding. The main content area is titled 'Destination Port Filtering' and contains the following elements:

- A descriptive text: 'Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.'
- A checkbox labeled 'Enable Destination Port Filtering'.
- Form fields for 'Port Range' (with a range selector), 'Protocol' (a dropdown menu currently set to 'Both'), and 'Comment'.
- 'Apply Changes' and 'Cancel' buttons.
- A section titled 'Current Filter Table' containing a table with the following headers: 'Dest Port Range', 'Protocol', 'Comment', 'Select', and 'Edit'.
- Below the table are buttons for 'Delete Selected', 'Delete All', and 'Cancel'.

Figure 22 Destination Port Filtering

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind IEEE 802.11N WIRELESS OUTDOOR CPE's NAT firewall.

The screenshot shows the 'Port Forwarding' configuration page. On the left is a sidebar with a menu: Basic Settings, IP Settings(Bridge), IP Settings(Router), RADIUS Settings, Time Settings, Firewall Settings, Src IP Filtering, Dest IP Filtering, Src Port Filtering, Dest Port Filtering, and Port Forwarding (highlighted with a double arrow). The main content area has a title 'Port Forwarding' and a descriptive paragraph: 'Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.' Below this is a form with fields: 'Enable Port Forwarding' (checkbox), 'IP Address' (text box), 'Protocol' (dropdown menu showing 'Both'), 'Port Range' (text box with a range separator), and 'Comment' (text box). At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a section titled 'Current Port Forwarding Table:' containing a table with headers: Local IP Address, Protocol, Port Range, Comment, Select, and Edit. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Cancel'.

Figure 23 Port Forwarding

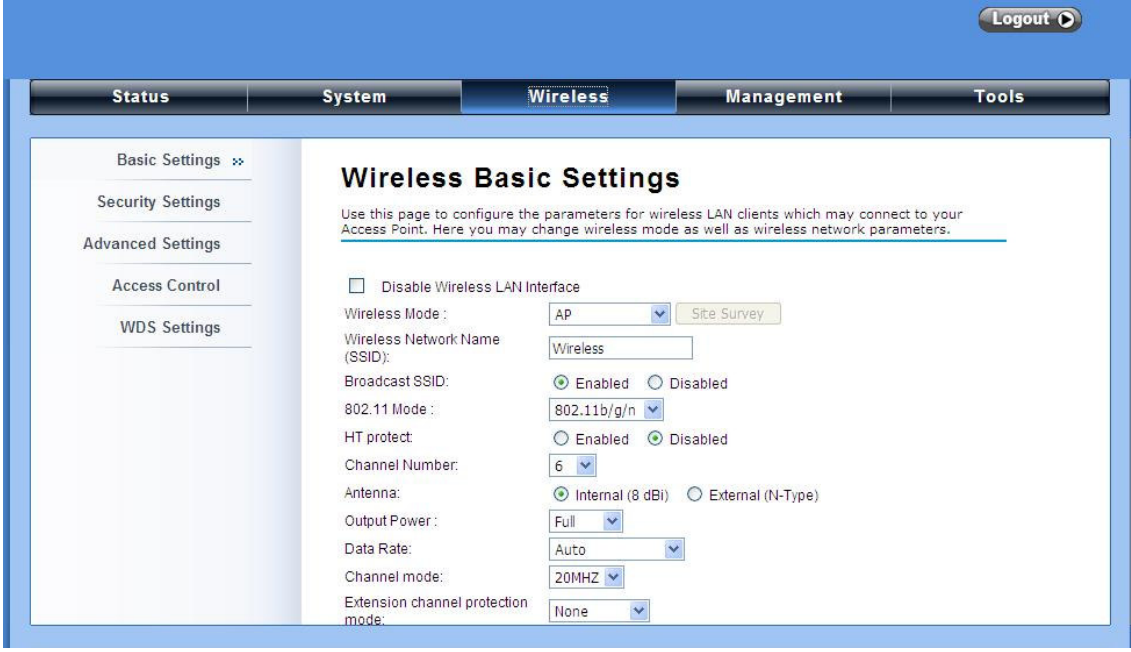
DMZ: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

The screenshot shows the 'DMZ' configuration page. The sidebar menu is identical to the previous screenshot, with 'DMZ' highlighted at the bottom. The main content area has a title 'DMZ' and a descriptive paragraph: 'A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers,SMTP (e-mail) servers and DNS servers.' Below this is a form with fields: 'Enable DMZ' (checkbox) and 'DMZ Host IP Address' (text box containing '0.0.0.0'). At the bottom of the form are 'Apply Changes' and 'Cancel' buttons.

Figure 24 DMZ

Basic Wireless Settings

Open “Basic Settings” in “Wireless” as below to make basic wireless configuration.



The screenshot shows a web interface for configuring wireless settings. At the top, there is a navigation bar with tabs: Status, System, Wireless (selected), Management, and Tools. A 'Logout' button is in the top right corner. On the left, a sidebar lists settings categories: Basic Settings (selected), Security Settings, Advanced Settings, Access Control, and WDS Settings. The main content area is titled 'Wireless Basic Settings' and includes a description: 'Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.' Below this, there are several configuration options: 'Disable Wireless LAN Interface' (checkbox), 'Wireless Mode' (dropdown menu set to 'AP' with a 'Site Survey' button), 'Wireless Network Name (SSID)' (text field set to 'Wireless'), 'Broadcast SSID' (radio buttons for 'Enabled' and 'Disabled'), '802.11 Mode' (dropdown menu set to '802.11b/g/n'), 'HT protect' (radio buttons for 'Enabled' and 'Disabled'), 'Channel Number' (dropdown menu set to '6'), 'Antenna' (radio buttons for 'Internal (8 dBi)' and 'External (N-Type)'), 'Output Power' (dropdown menu set to 'Full'), 'Data Rate' (dropdown menu set to 'Auto'), 'Channel mode' (dropdown menu set to '20MHZ'), and 'Extension channel protection mode' (dropdown menu set to 'None').

Figure 16 Basic Wireless Settings

- **Disable Wireless LAN Interface**

Check this option to disable WLAN interface, then the wireless module of IEEE 802.11N WIRELESS OUTDOOR CPE will stop working and no wireless device can connect to it.

- **Wireless Mode**

Four operating modes are available on IEEE 802.11N WIRELESS OUTDOOR CPE.

Wireless Client: The IEEE 802.11N WIRELESS OUTDOOR CPE is able to connect to the AP and thus join the wireless network around it.

AP: The IEEE 802.11N WIRELESS OUTDOOR CPE establishes a wireless coverage and receives connectivity from other wireless devices.

Bridge: The IEEE 802.11N WIRELESS OUTDOOR CPE establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the “WDS Setting” for detailed configuration.

AP Repeater: The IEEE 802.11N WIRELESS OUTDOOR CPE servers as AP and Bridge concurrently. In other words, the IEEE 802.11N WIRELESS OUTDOOR CPE can provide connectivity services for CPEs under WDS mode.

- **Wireless Network Name (SSID)**

This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

- **Broadcast SSID**

Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA can not scan and find IEEE 802.11N WIRELESS OUTDOOR CPE, so that malicious attack by some illegal STA could be avoided.

- **802.11 Mode**

The IEEE 802.11N WIRELESS OUTDOOR CPE can communicate with wireless devices of 802.11b/g or 802.11b/g/n. You can also select Auto and make it work under an appropriate wireless mode automatically.

- **HT Protect**

Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

- **Channel Number**

Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Antenna**

By default, IEEE 802.11N WIRELESS OUTDOOR CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from “Internal (8 dBi)” to “External (N-Type)”.



Note:

-
- You are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11N WIRELESS OUTDOOR CPE itself.
-

- **Output Power**

Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually “Full” is preferred.

- **Data Rate**

Usually “**Auto**” is preferred. Under this rate, the IEEE 802.11N WIRELESS OUTDOOR CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Channel Mode**

Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

- **Extension Channel Protection Mode**

This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

- **Enable MAC Clone**

Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

Site Survey

Under wireless client mode, the IEEE 802.11N WIRELESS OUTDOOR CPE is able to perform site survey, through which, information on the available access points will be detected.

Open “**Basic Settings**” in “**Wireless**”, by clicking the “**Site Survey**” button beside “**Wireless Mode**” option, the wireless site survey window will popup with a list of available wireless networks around. Select the AP you would like to connect and click “**Selected**” to establish connection. The wireless site survey window can also be viewed by opening the “**Site Survey**” page in “**Tools**”.

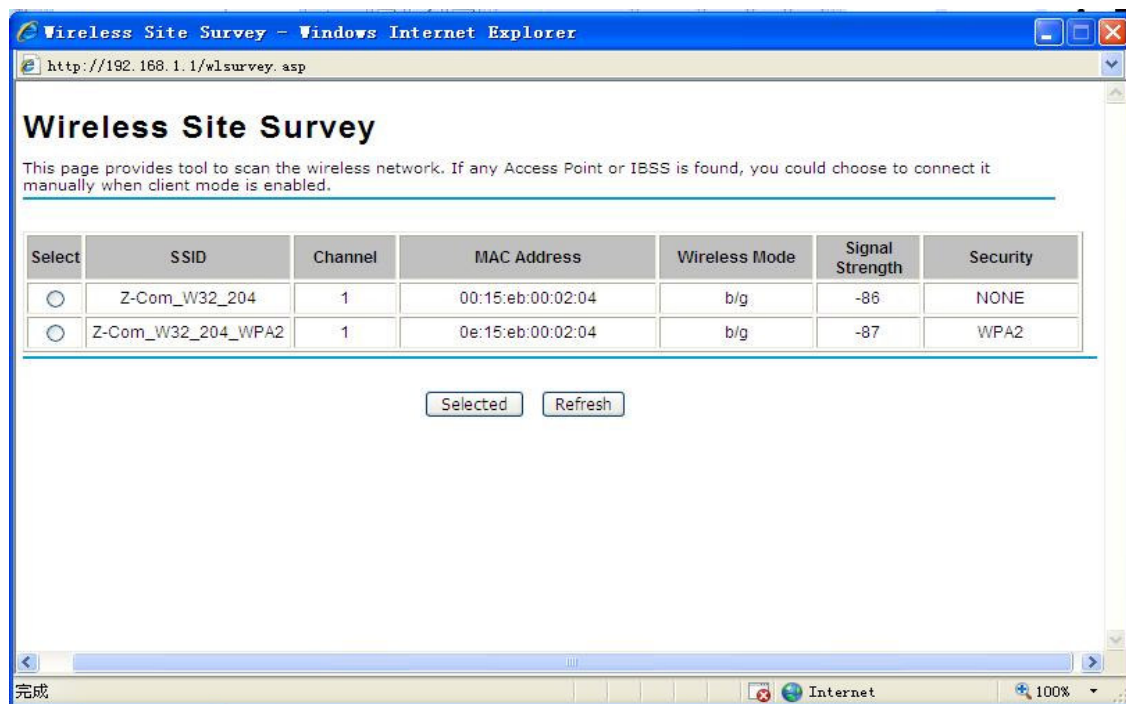


Figure 17 Site Survey

Chapter 4 Advanced Settings

Advanced Wireless Settings

Open “**Advanced Settings**” in “**Wireless**” to make advanced wireless settings.

The screenshot shows a web-based network management interface. At the top, there is a blue header bar with a "Logout" button. Below the header is a navigation menu with tabs: "Status", "System", "Wireless", "Management", and "Tools". The "Wireless" tab is selected. On the left side of the "Wireless" tab, there is a sidebar menu with options: "Basic Settings", "Security Settings", "Advanced Settings" (which is highlighted with a double arrow), "Access Control", and "WDS Settings". The main content area displays the "Advanced Wireless Settings" configuration. It includes various settings with radio buttons for enabling or disabling features and input fields for numerical values. The settings are: WMM Support (Enabled), A-MPDU aggregation (Enabled), A-MSDU aggregation (Disabled), Short GI (Enabled), RTS Threshold (2346), Fragment Threshold (2346), Beacon Interval (100), DTIM Interval (1), Preamble Type (Short), IGMP Snooping (Enabled), Wireless Separation (Disabled), RIFS (Enabled), Link Intergration (Disabled), Max. Station Num (32), Space In Meter (0), and ACK Timeout (100).

Setting	Value	Range/Options
WMM Support	Enabled	Enabled / Disabled
A-MPDU aggregation	Enabled	Enabled / Disabled
A-MSDU aggregation	Disabled	Enabled / Disabled
Short GI	Enabled	Enabled / Disabled
RTS Threshold	2346	(1-2346)
Fragment Threshold	2346	(256-2346)
Beacon Interval	100	(20-1024 ms)
DTIM Interval	1	(1-255)
Preamble Type	Short	Long / Short
IGMP Snooping	Enabled	Enabled / Disabled
Wireless Separation	Disabled	Enabled / Disabled
RIFS	Enabled	Enabled / Disabled
Link Intergration	Disabled	Enabled / Disabled
Max. Station Num	32	(0-32)
Space In Meter	0	(0-100000m)
ACK Timeout	100	(100-767 microsecond)

Figure 18 Advanced Wireless Settings

- **WMM Support**

WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it.

- **A-MPDU/A-MSDU Aggregation**

The data rate of your AP except wireless client mode, could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

- **Short GI**

Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

- **RTS Threshold**

The IEEE 802.11N WIRELESS OUTDOOR CPE sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Fragmentation Length**

Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

- **DTIM Interval**

DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

- **Preamble Type**

It defines some details on the 802.11 physical layer. “**Long**” and “**Short**” are available.

- **IGMP Snooping**

IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

- **Wireless Separation**

Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except wireless client mode, enable “**Wireless Separation**” can prevent the communication among associated wireless clients.

- **RIFS**

RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

- **Link Integration**

Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking “**Enabled**”. It can inform the associating wireless clients as soon as the disconnection occurs.

- **Max. Station Num**

Available only under AP mode, it defines the maximum amount of wireless clients allowed to be connected.

- **Space in Meter/ACK Timeout**

To decrease the chances of data retransmission at long distance, the IEEE 802.11N WIRELESS OUTDOOR CPE can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

- **Flow Control**

It allows the administrator to specify the incoming and outgoing traffic limit by checking “**Enable Traffic Shaping**”. This is only available in Router mode.

 Note:

-
- We strongly recommend you leave most advanced settings at their defaults except “Distance in Meters” adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.
-

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11N WIRELESS OUTDOOR CPE provides you with rock solid security settings.

Security Settings

Open “Security Settings” in “Wireless” as below:

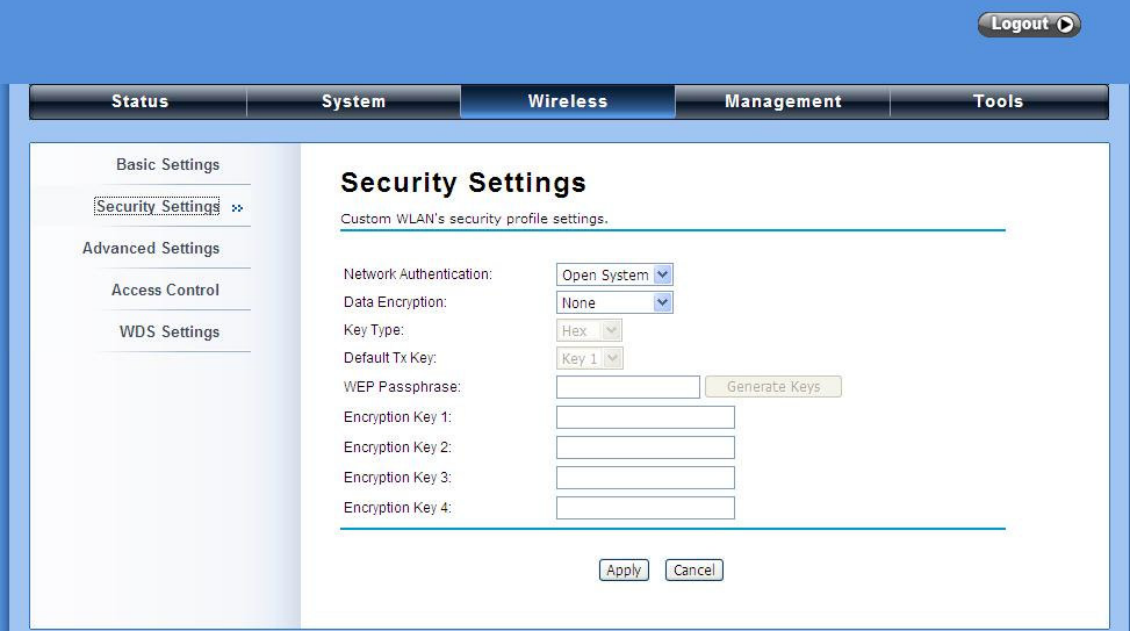
The screenshot shows a web interface for configuring wireless security. At the top, there is a blue header bar with a 'Logout' button. Below the header is a navigation menu with tabs for 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'Wireless' tab is selected. On the left side, there is a sidebar with a tree view containing 'Basic Settings', 'Security Settings' (which is expanded and highlighted with a double arrow), 'Advanced Settings', 'Access Control', and 'WDS Settings'. The main content area is titled 'Security Settings' and contains the text 'Custom WLAN's security profile settings.' Below this, there are several configuration fields: 'Network Authentication' (a dropdown menu set to 'Open System'), 'Data Encryption' (a dropdown menu set to 'None'), 'Key Type' (a dropdown menu set to 'Hex'), and 'Default Tx Key' (a dropdown menu set to 'Key 1'). To the right of the 'WEK Passphrase' field is a 'Generate Keys' button. Below these are four text input fields for 'Encryption Key 1', 'Encryption Key 2', 'Encryption Key 3', and 'Encryption Key 4'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 19 Security Settings

- **Network Authentication**

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication.

Legacy 802.1x: As an IEEE standard for port-based Network Access Control, it provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

WPA with RADIUS: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.

WPA&WPA2 with RADIUS: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.



Note:

-
- We strongly recommend you enable wireless security on your network!
 - Only setting the same Authentication, Data Encryption and Key in the IEEE 802.11N WIRELESS OUTDOOR CPE and other associated wireless devices, can the communication be established!
-

Access Control

The Access Control appoints the authority to wireless client on accessing IEEE 802.11N WIRELESS OUTDOOR CPE, thus a further security mechanism is provided. This function is available only under AP mode.

Open “**Access Control**” in “**Wireless**” as below.

The screenshot shows a web interface for configuring wireless access control. At the top, there is a navigation bar with tabs: Status, System, Wireless (selected), Management, and Tools. A 'Logout' button is in the top right corner. On the left, a sidebar lists settings categories: Basic Settings, Security Settings, Advanced Settings, Access Control (selected with a double arrow), and WDS Settings. The main content area is titled 'Wireless Access Control'. It contains a text block explaining the 'Allowed Listed' and 'Deny Listed' modes. Below this, there is a form with 'Access Control Mode' set to 'Disable' and an empty 'MAC Address' field. 'Apply' and 'Cancel' buttons are present. At the bottom, there is a table with a header 'MAC Address' and buttons 'Select' and 'Edit'. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Refresh'.

Figure 20 Access Control

- **Access Control Mode**

If you select “**Allow Listed**”, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “**Deny Listed**” is selected, those wireless clients on the list will not be able to connect the AP.

- **MAC Address**

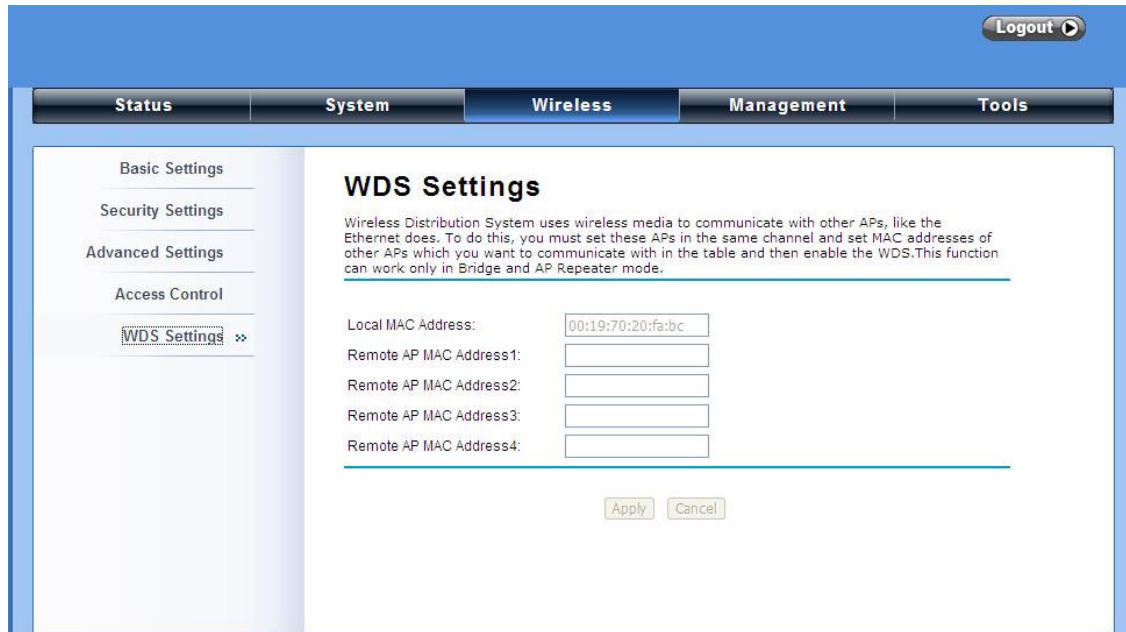
Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.

- **Delete Selected/All**

Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click “**Delete Selected**” or “**Delete All**” to cancel that access control rule.

WDS Settings

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Simply put, you can link the Access Points wirelessly. Open “WDS Settings” in “Wireless” as below:



The screenshot shows a web-based network management interface. At the top right is a "Logout" button. Below it is a navigation bar with tabs: "Status", "System", "Wireless", "Management", and "Tools". The "Wireless" tab is selected. On the left side, there is a sidebar menu with categories: "Basic Settings", "Security Settings", "Advanced Settings", and "Access Control". Under "Advanced Settings", "WDS Settings" is highlighted with a double arrow. The main content area is titled "WDS Settings". It contains a descriptive paragraph: "Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS. This function can work only in Bridge and AP Repeater mode." Below this text is a table with five rows: "Local MAC Address:" (with a text box containing "00:19:70:20:fa:bc"), "Remote AP MAC Address1:", "Remote AP MAC Address2:", "Remote AP MAC Address3:", and "Remote AP MAC Address4:". Each row has an empty text box for input. At the bottom of the form are "Apply" and "Cancel" buttons.

Figure 30 WDS Settings

Enter the MAC address of another AP you wirelessly want to connect to into the appropriate field and click “**Apply**” to save settings.

 Note:

- WDS Settings is available only under Bridge and AP Repeater Mode.

Chapter 5 Management

SNMP Management

The IEEE 802.11N WIRELESS OUTDOOR CPE supports SNMP for convenient remote management. Open “**SNMP Configuration**” in “**Management**” shown below. Set the SNMP parameters and obtain MIB file before remote management.

The screenshot shows a web management interface for an IEEE 802.11N WIRELESS OUTDOOR CPE. At the top, there is a blue header bar with a "Logout" button. Below this is a navigation menu with tabs for "Status", "System", "Wireless", "Management", and "Tools". The "Management" tab is selected. On the left side of the "Management" section, there is a sidebar with links: "SNMP Configuration" (highlighted with a double arrow), "Password Settings", "Firmware Upload", and "Configuration File". The main content area is titled "SNMP Configuration" and includes the instruction "Use this page to set SNMP settings." Below this, there is a section for "Enable SNMP" with a checked checkbox. Underneath, several configuration fields are listed: "Protocol Version" (a dropdown menu set to "V3"), "Server Port" (a text box containing "161"), "Get Community" (a text box containing "public"), "Set Community" (a text box containing "private"), "Trap Destination" (a text box containing "0.0.0.0"), and "Trap Community" (a text box containing "public"). At the bottom of the configuration area, there is a link "Configure SNMPv3 User Profile" and two buttons, "Apply" and "Cancel".

Figure 31 SNMP Configuration

- **Enable SNMP**

Check this box to enable SNMP settings.

- **Protocol Version**

Select the SNMP version, and keep it identical on the IEEE 802.11N WIRELESS OUTDOOR CPE and the SNMP manager.

- **Server Port**

Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

- **Get Community**

Specify the password for the incoming Get and GetNext requests from the management station. By

default, it is set to public and allows all requests.

- **Set Community**

Specify the password for the incoming Set requests from the management station. By default, it is set to private.

- **Trap Destination**

Specify the IP address of the station to send the SNMP traps to.

- **Trap Community**

Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Configure SNMPv3 User Profile

For SNMP protocol version 3, you can click “**Configure SNMPv3 User Profile**” in blue to set the details of SNMPv3 user. Check “**Enable SNMPv3 Admin/User**” in advance and make further configuration.

Figure 32 Configure SNMPv3 User Profile

- **User Name**

Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the IEEE 802.11N WIRELESS OUTDOOR CPE.

- **Password**

Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this

password are allowed to access the IEEE 802.11N WIRELESS OUTDOOR CPE.

- **Confirm Password**

Input that password again to make sure it is your desired one.

- **Access Type**

Select “**Read Only**” or “**Read and Write**” accordingly.

- **Authentication Protocol**

Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

- **Privacy Protocol**

Specify the encryption method for SNMP communication. None and DES are available.

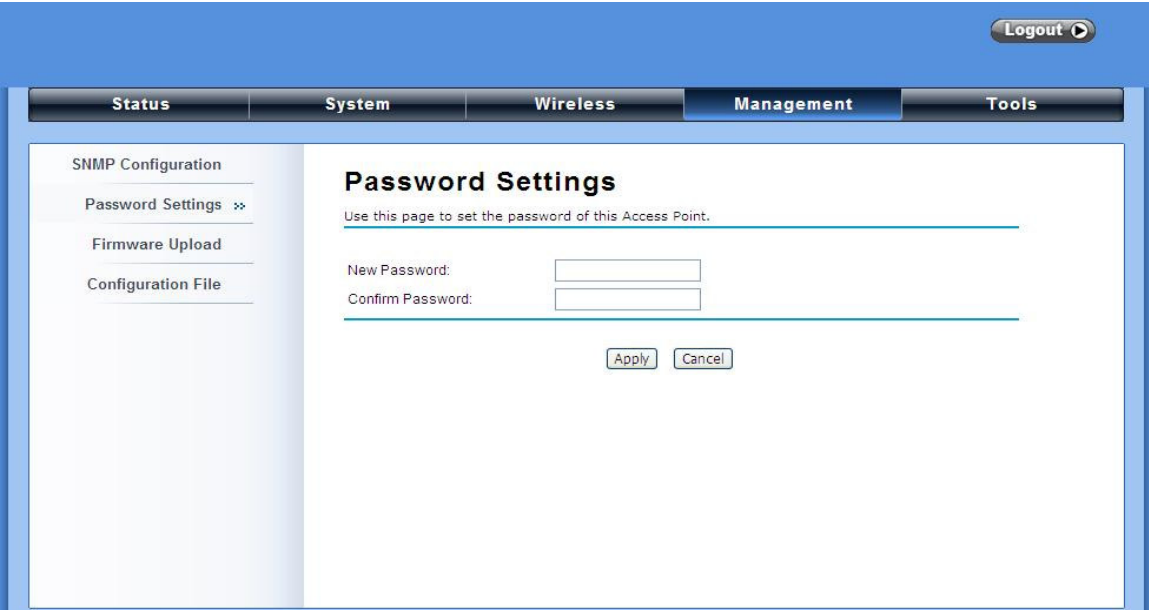
None: No encryption is applied.

DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Password

From “**Password Settings**” in “**Management**”, you can change the password to manage your IEEE 802.11N WIRELESS OUTDOOR CPE.

Enter the new password respectively in “**New Password**” and “**Confirm Password**” fields; click “**Apply**” to save settings.



The screenshot shows a web interface with a blue header and a navigation bar. The navigation bar has tabs for Status, System, Wireless, Management, and Tools. The Management tab is selected. On the left, there is a sidebar with links for SNMP Configuration, Password Settings (selected), Firmware Upload, and Configuration File. The main content area is titled "Password Settings" and contains the instruction "Use this page to set the password of this Access Point." Below this, there are two input fields: "New Password:" and "Confirm Password:". At the bottom of the form, there are "Apply" and "Cancel" buttons. A "Logout" button is visible in the top right corner of the interface.

Figure 33 Password

 Note:

- The password is case-sensitive and its length can not be exceed 19 characters!

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through IEEE 802.11N WIRELESS OUTDOOR CPE’s Web:

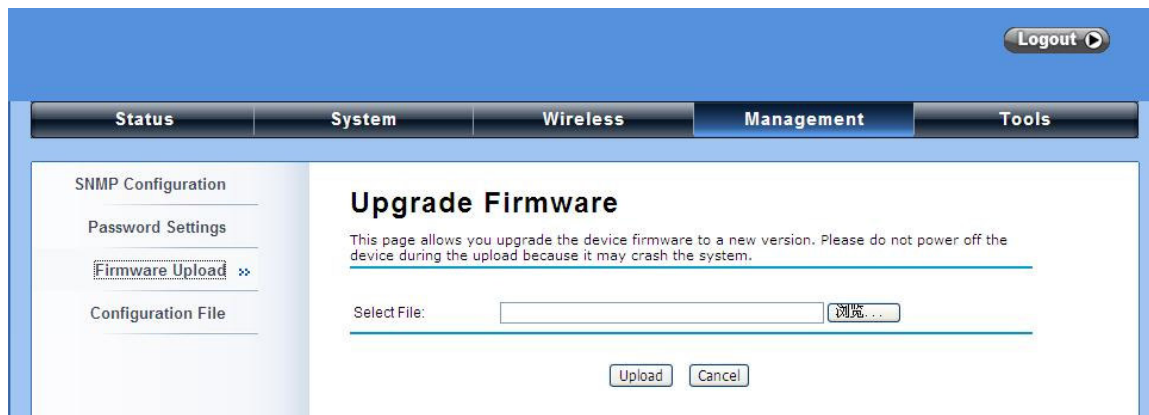


Figure 34 Upgrade Firmware

- Click “**Browse**” to select the firmware file you would like to load;
- Click “**Upload**” to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

 Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open “**Configuration File**” in “**Management**” as below:

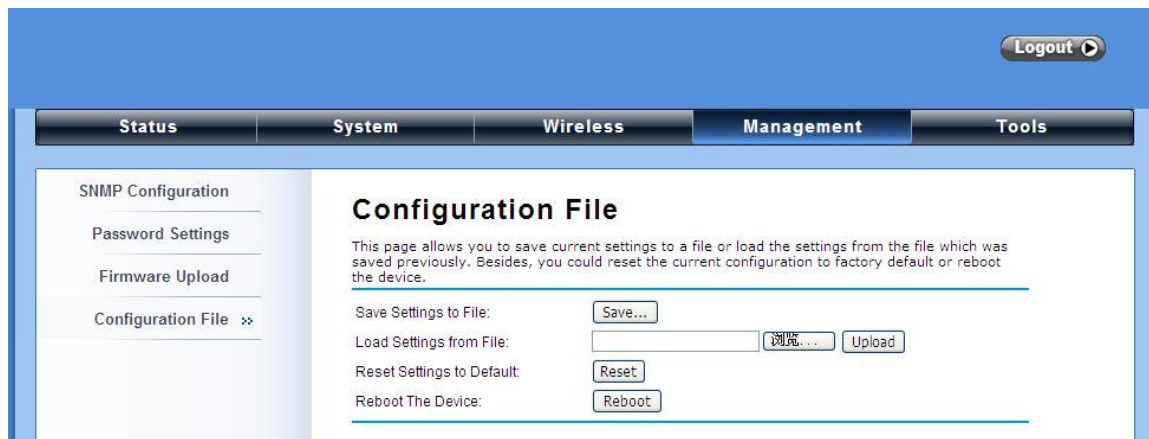


Figure 35 Backup/Retrieve Settings

- **Backup Settings**

By clicking “**Save**”, a dialog box will pop up. Save it, then the configuration file like **ap.cfg** will be saved to your local computer.

- **Retrieve Settings**

By clicking “**Browse**”, a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click “**Upload**” to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The IEEE 802.11N WIRELESS OUTDOOR CPE provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

From “**Configuration File**”, clicking “**Reset**” will eliminate all current settings and reboot your device, then default settings are applied.

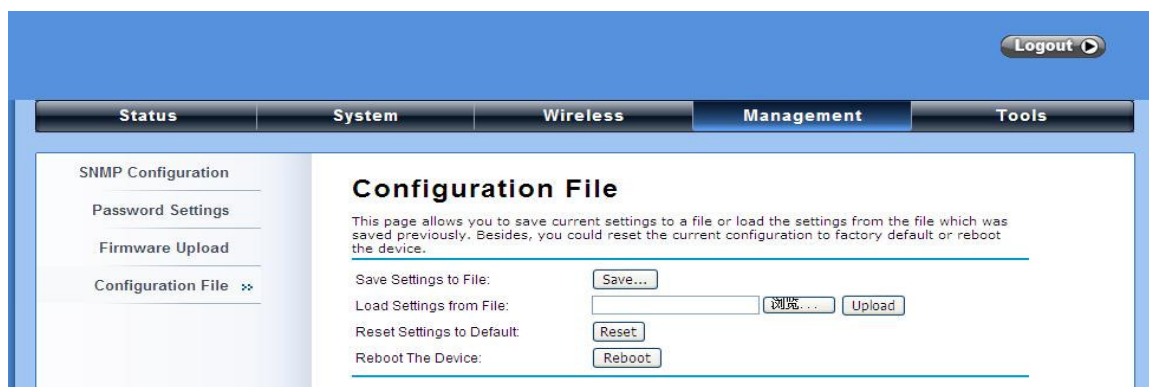


Figure 21 Restore Settings

- **Restore factory default settings via Reset Button**

If software in IEEE 802.11N WIRELESS OUTDOOR CPE is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

Reboot

You can reboot your IEEE 802.11N WIRELESS OUTDOOR CPE from “**Configuration File**” in “**Management**” as below:

Click “**Reboot**” and hit “**Yes**” upon the appeared prompt to start reboot process. This takes a few minutes.

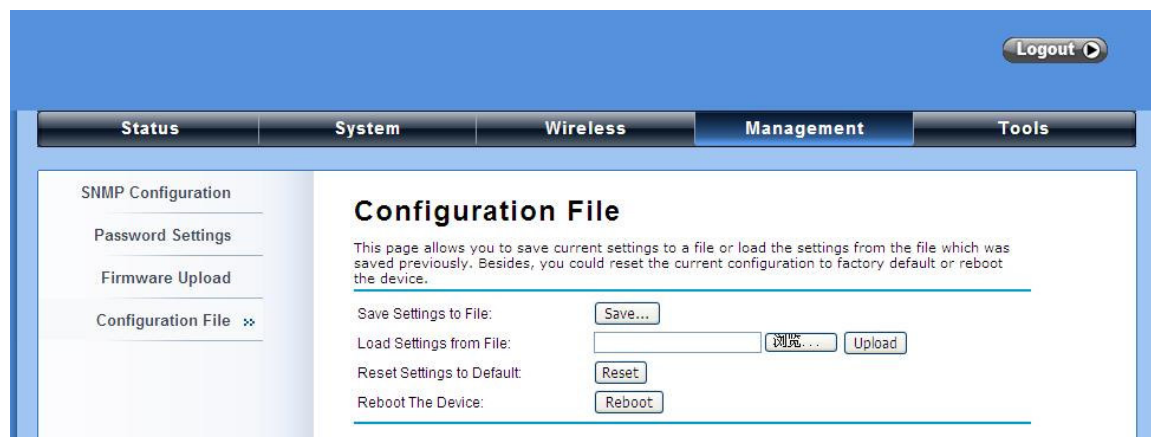


Figure 37 Reboot

System Log

System log is used for recording events occurred on the IEEE 802.11N WIRELESS OUTDOOR CPE, including station connection, disconnection, system reboot and etc.

Open “**System Log**” in “**Tools**” as below.

Wireless Broadband Access Point

Logout

Status

System

Wireless

Management

Tools

System Log

Site Survey

Ping Watchdog

System Log

Use this page to set remote log server and show the system log.

Remote Syslog Server:

Enable Remote Syslog

IP Address

0.0.0.0

Port

514

Apply

Cancel

#	Time	Source	Message
1	00:00:18	00:19:70:27:EB:E7	WLAN service stopped.
2	00:00:18	00:19:70:27:EB:E7	WLAN service started.
3	00:00:18	00:19:70:27:EB:E7	WLAN service stopped.
4	00:00:18	00:19:70:27:EB:E7	WLAN service started.
5	00:00:18	00:19:70:27:EB:E7	WLAN service stopped.
6	00:00:19	00:19:70:27:EB:E7	WLAN service started.
7	00:00:19	00:19:D2:99:5E:1A	Station associated.
8	00:00:19	00:19:D2:99:5E:1A	Station disassociated.

Figure 38 System Log

- Remote Syslog Server

Enable Remote Syslog: Enable System log to alert remote server.

IP Address: Specify the IP address of the remote server.

Port: Specify the port number of the remote server.

Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage.

Open “**Site Survey**” in “**Tools**” as below and select the desired AP to connect.

Wireless Broadband Access Point

Logout

Status

System

Wireless

Management

Tools

System Log

Site Survey >>

Ping Watchdog

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security
☐	MISVOIP	1	00:60:b3:35:92:59	b/g	-68	WEP
☐	7F-MIS	11	00:0fb5:03:ff:82	b/g	-47	NONE
☐	sirius	11	00:21:a0:03:b8:c0	b/g	-95	WPA
☐	MIS-AP1	10	00:07:40:e8:ae:8e	b/g	-69	NONE
☐	sirius	1	00:21:a0:03:b3:b0	b/g	-98	WPA

Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.

Wireless Broadband Access Point

Logout

Status

System

Wireless

Management

Tools

System Log

Site Survey

Ping Watchdog >>

Ping Watchdog

This page provides a tool to configure the Ping Watchdog. If the failcount of the Ping reaches to a specified value, the watchdog will reboot the device.

☒ Enable Ping Watchdog

IP Address to Ping

Ping Interval
 seconds

Startup Delay
 seconds

Failure Count To Reboot

- **Ping Watchdog**

Enable Ping Watchdog: To activate ping watchdog, check this checkbox.

IP Address to Ping: Specify the IP address of the remote unit to ping.

Ping Interval: Specify the interval time to ping the remote unit.

Startup Delay: Specify the startup delay time to prevent reboot before the IEEE 802.11N WIRELESS OUTDOOR CPE is fully initialized.

Failure Count To Reboot: If the ping timeout packets reached the value, the IEEE 802.11N WIRELESS OUTDOOR CPE will reboot automatically.

Chapter 6 Status

View IEEE 802.11N WIRELESS OUTDOOR CPE Basic Information

Open “**Information**” in “**Status**” to check the basic information of IEEE 802.11N WIRELESS OUTDOOR CPE, which is read only. Click “**Refresh**” at the bottom to have the real-time information.



Figure 22 Basic Information

View Association List

Open “**Association List**” in “**Connection**” from “**Status**” to check the information of associated wireless clients. All is read only. Click “**Refresh**” at the bottom to view the current association list.

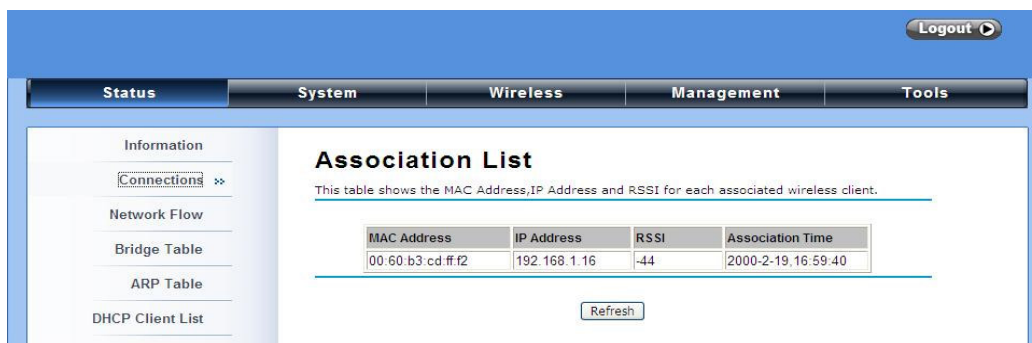


Figure 23 Connection

View Network Flow Statistics

Open “**Network Flow**” in “**Status**” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “**Refresh**” to view current statistics.

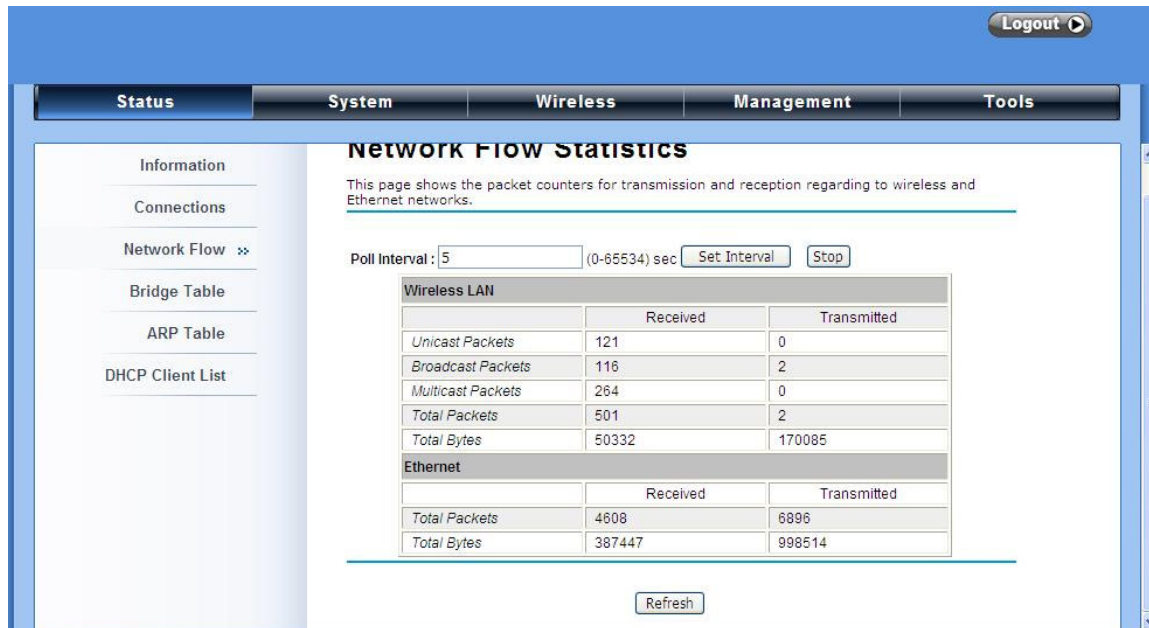


Figure 24 Network Flow Statistics

● Poll Interval

Specify the refresh time interval in the box beside “**Poll Interval**” and click “**Set Interval**” to save settings. “**Stop**” helps to stop the auto refresh of network flow statistics.

View Bridge Table

Open “**Bridge Table**” in “**Status**” as below. Click “**Refresh**” to view current connected status..

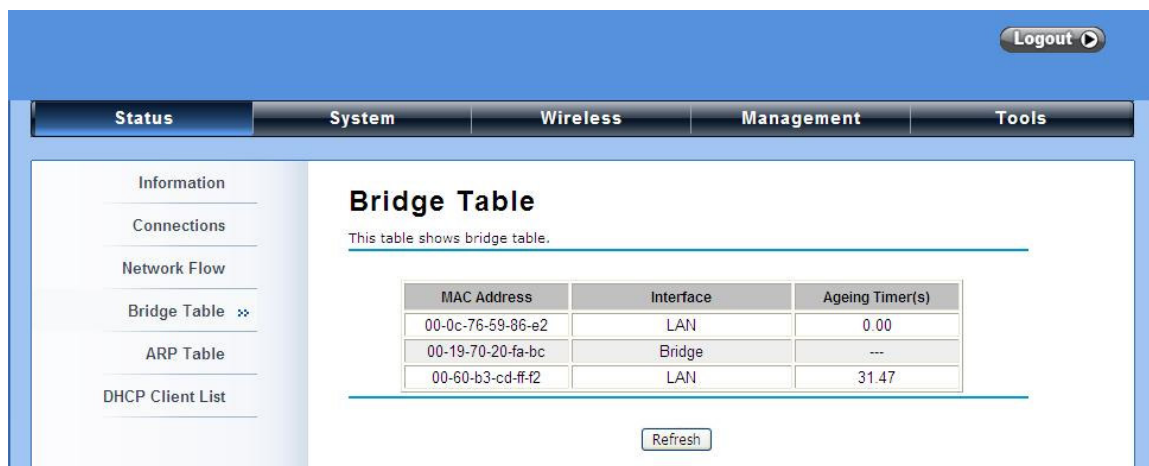


Figure 42 Bridge Table

View ARP Table

Open "ARP Table" in "Status" as below. Click "Refresh" to view current table.

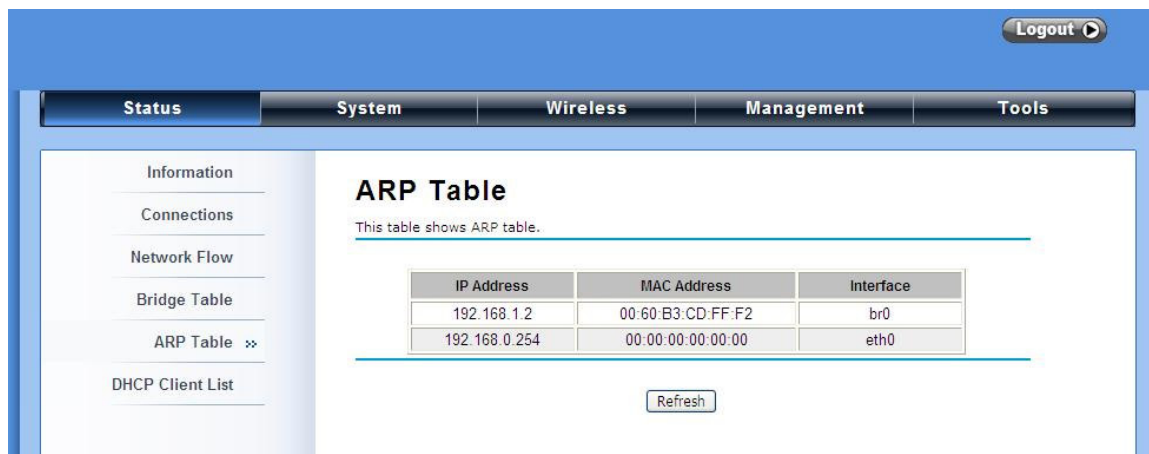


Figure 43 ARP Table

View Active DHCP Client Table

Open “**DHCP Client List**” in “**Status**” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “**Refresh**” to view current table.



Figure 44 DHCP Client Table

Chapter 7 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the IEEE 802.11N WIRELESS OUTDOOR CPE. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of IEEE 802.11N WIRELESS OUTDOOR CPE?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

- Each device has a label posted with the MAC address. Please refer below.

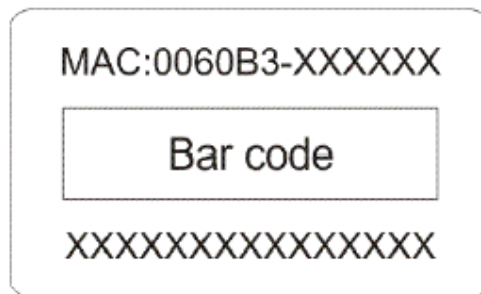


Figure 25 MAC Address

- On the IEEE 802.11N WIRELESS OUTDOOR CPE Web-based management interface, you can view the MAC Address from [“View IEEE 802.11N WIRELESS OUTDOOR CPE Basic Information”](#).

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in **“Configuration File”** from **“Management”**.

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in **“Configuration File”** from **“Management”**.

Q 4. What if I can not access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.

- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the IEEE 802.11N WIRELESS OUTDOOR CPE comes with a built-in directional antenna, it is recommended make the IEEE 802.11N WIRELESS OUTDOOR CPE face to the direction where the AP is to get the best connection quality.
- In addition, you can start **"Site Survey"** in **"Wireless Basic Settings"** to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.

Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ASCII).

As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 2 ASCII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64		7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Appendix B. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there may contains some public software, if it is, please read below carefully:

1. Definition

“**Public Software**”, when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found.

“Public Software” shall mean each of:

- (a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and
- (b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU’s General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2.

Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and

conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table 3 Public Software Name and Description

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
Redboot	Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.	ftp://ftp.gnu.org/ftp.gnu.com/private/gnupro-xscale-030422/redboot-intel-xscale-030630.tar.gz	eCos License	http://sources.redhat.com/ecos/ecos-license/
Busybox		http://www.busybox.net/downloads/busybox-1.01.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
brctl	Copyright (C) 2000	http://nchc	GNU GENERAL PUBLIC	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

	Lennert Buytenhek	.dl.sourceforge.net/sourceforge/bridge/bridge-utils-1.0.6.tar.gz	LICENSE Version 2	rg/licenses/old-licenses/gpl-2.0.html
dropbear	Copyright (c) 2002-2006 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu	http://matt.ucc.asn.au/dropbear/dropbear-0.51.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
hostapd	Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
wpa_supplicant	Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
mtddutil		ftp://ftp.uk.linux.org/pub/people/dwmw2/mtdd/cvs/mtddutil/	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ntpclient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icarus.com/ntpclient/ntpclient_2003_194.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
procps	Author: Albert Cahalan, Michael K. Johnson, Jim Warner, etc.	http://procps.sourceforge.net/procps-3.2.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2 GNU LIBRARY GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html http://www.gnu.org/licenses/old-licenses/library.html

vsftpd	Author: Chris Evans	ftp://vsftpd.beasts.org/users/chris-evans/vsftpd-1.1.2.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.20.3.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html